What is Claimed is:

1. A packet-based encryption system comprising:

a transmitting device to encrypt data and to insert a pseudo-random key in a transmitted packet; and

a receiving device to receive and to decrypt said data in said transmitted packet using said pseudo-random key.

2. The system of claim 1 wherein said transmitting device further comprises:

means to generate a random number;

a first one-way cryptographic hash function means to generate a hashed number from said random number;

a first streaming cipher algorithm using a seed to encrypt said hashed number;

encryption means to encrypt said data using results of said first streaming cipher algorithm; and

means to insert said random number in a specified field of said transmitted packet.

3. The system of claim 2 wherein said receiving device further comprises:

means to remove said random number from said specified field of said transmitted packet;

a second one-way cryptographic hash function means to generate a second hashed number from said random number;

a second streaming cipher algorithm using a seed to encrypt said second hashed number; and

decryption means to decrypt said data using results of said second streaming cipher algorithm.

4. The system of claim 3 wherein said first one-way cryptographic hash function and said second one-way cryptographic hash function use the same algorithm and use a same first seed or key.

5. The system of claim 4 wherein said first streaming cipher algorithm and said second streaming cipher algorithm are the same and use a same second seed or key.

6. The system of claim 5 wherein said encryption means and said decryption means use the same third key and algorithm.

7. The system of claim 1 wherein said transmitting device further comprises:

means to generate a random number;

a first one-way cryptographic hash function means to generate a hashed number from said random number;

a third one-way cryptographic hash function using a seed to encrypt said hashed number;

encryption means to encrypt said data using results of said third one-way cryptographic hash function; and

means to insert said random number in a specified field of said transmitted packet.

8. The system of claim 7 wherein said receiving device further comprises:

means to remove said random number from said specified field of said transmitted packet;

a second one-way cryptographic hash function means to generate a second hashed number from said random number;

a fourth one-way cryptographic hash function using a seed to encrypt said second hashed number; and

decryption means to decrypt said data using results of said fourth one-way cryptographic hash function.

9. The system of claim 8 wherein said third one-way cryptographic hash function and said fourth one-way cryptographic hash function are the same and use a same fourth seed or key.

10. A method of encryption of packetized data using a symmetric key-based stream cipher, in which each packet includes self-synchronizing information comprising the steps of:

encrypting data and inserting a pseudo-random key in a transmitted packet with said encrypted data; and

decrypting said data in said transmitted packet with said inserted pseudo-random key.

11. The method of claim 10 further comprising the steps of:

at the transmitting end:

- generating a random number;
- generating a hashed number from said random number using a first one-way cryptographic hash function;
- providing a first streaming cipher algorithm using said hashed number as a seed;
- encrypting said data using results of said first streaming cipher algorithm; and
- inserting said random number in a specified field of said transmitted packet.

at the receiving end:

- removing said random number from said specified field of said transmitted packet;
- generating a second hashed number from said random number using a second one-way cryptographic hash function;

- providing a second streaming cipher algorithm using said hashed number as a seed; and

- decrypting said data using results of said second streaming cipher algorithm using said second hashed number as a seed.

12. The method of claim 10 further comprising the steps of:

at the transmitting end:

- generating a random number;

- generating a hashed number from said random number using a first one-way cryptographic hash function;

- providing a third one-way cryptographic hash function using a seed to encrypt sâid hashed number;

- encrypting said data using results of said first streaming cipher algorithm; and

- inserting said random number in a specified field of said transmitted packet.

at the receiving end:

- removing said random number from said specified field of said transmitted packet;

- generating a second hashed number from said random number using a second one-way cryptographic hash function;

- providing a fourth one-way cryptographic hash function using a seed to encrypt said second hashed number; and

- decrypting said data using results of said second streaming cipher algorithm using said second hashed number as a seed.